AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning at line 24 on page 6 of the substitute specification with the following rewritten paragraph.

The object of the present invention is achieved by a cryptocommunication system including a transmission apparatus and a reception apparatus. The transmission apparatus encrypts plaintext to generate ciphertext, performs a one-way operation on the plaintext to generate a first value, and transmits the ciphertext and the first value to the reception apparatus. The reception apparatus receives the ciphertext and the first value, decrypts the ciphertext to generate decrypted text, performs the one-way operation on the decrypted text to generate a second value, and judges that the decrypted text matches the plaintext when the second value and the first value match. The transmission apparatus includes: a first generating unit for generating first additional information; a first operation unit for performing an invertible operation on the plaintext and the first additional information to generate connected information; an encrypting unit for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext; and a transmitting unit for transmitting the ciphertext. The reception apparatus comprises: a receiving unit for receiving the ciphertext; a second generating unit for generating second additional information which is ~~dentical~~ identical to the first additional information; a decrypting unit for decrypting the ciphertext according to a decryption algorithm, which is an inverse-conversion of the encryption algorithm, so as to generate decrypted connected information; and a second operation unit for performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.

Please replace the paragraph beginning at line 5 on page 12 of the substitute specification with the following rewritten paragraph.

The cryptocommunication system 1 uses the NTRU ~~cyrptosystem~~ cryptosystem which is one of the decryption error vulnerable cryptosystems. Please refer to Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem," Lecture Notes in Computer Science, 1423, pp. 267-288, Springer-Verlag, 1998 for a detailed description about a method of generating NTRU ciphertext, and a method of generating an encryption key and a decryption key for the NTRU cryptosystem.

Please replace the paragraph beginning at line 13 on page 14 of the substitute specification with the following rewritten paragraph.

Here, the one-way operation is a function which is designed to calculate a value from an inputted value, and which makes it difficult to calculate the originally inputted value from the value. Further, an assumption is made about the hash function h used here that it is assured to be difficult enough to obtain a value for the plaintext m by using the value h(m), and it is collide-free. For the details of the one-way operation, the hash function, the security of the hash function, and the collision-free ~~charasteristic~~ characteristic of the hash function, refer to Tatsuaki Okamoto, Hirosi Yamamoto, "Gendai Ango"(Modern cryptography), Series/Mathematics in Information Science, Sangyo-Tosho, 1997,pp.56, and pp.189-195.

Please replace the paragraph beginning at line 5 on page 15 of the substitute specification with the following rewritten paragraph.

As ~~hown~~ shown in FIG. 2, the encrypting unit 105 consists of a random number generation unit 1051, an encryption key storage 1052, and an encryption function unit 1053.

Please replace the paragraph beginning at line 3 on page 31 of the substitute specification with the following rewritten paragraph.

The following is a description on modification examples for the ~~cyrptocommunication~~ cryptocommunication system 1 in which additional information is shared.